

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA	:	No. 1:22-cr-383
	:	
v.	:	(Judge Conner)
	:	
DONNIE WOODS,	:	
Defendant	:	Electronically filed

**UNITED STATES' BRIEF IN
OPPOSITION TO MOTION TO SUPPRESS**

GERARD M. KARAM
United States Attorney

Carlo D. Marchioli
Assistant U.S. Attorney
PA 309217
United States Attorney's Office
Middle District of Pennsylvania
Sylvia H. Rambo U.S. Courthouse
1501 North 6th Street, Box 202
Harrisburg, PA 17102
Tel: (717) 221-4482
carlo.d.marchioli@usdoj.gov

March 12, 2024

TABLE OF CONTENTS

PROCEDURAL AND FACTUAL BACKGROUND	1
QUESTIONS PRESENTED.....	6
ARGUMENT	6
I. The good-faith exception precludes suppression of electronically stored evidence possessed and provided by a third party	6
II. The good-faith exception precludes suppression because the omission of section II from Attachment B was due to a clerical error.....	11
III. The good-faith exception precludes suppression because a reasonable officer would have believed that he could seize all of the data provided by Apple.....	18
IV. Severance or redaction is the only appropriate remedy	22
V. Evidence obtained pursuant to subsequent warrants should not be suppressed.....	24
CONCLUSION	34

TABLE OF AUTHORITIES

<u>Cases</u>	Page(s)
<i>Arizona v. Evans</i> , 514 U.S. 1 (1995)	13
<i>Carpenter v. United States</i> , 585 U.S. 296 (2018)	8
<i>Davis v. United States</i> , 564 U.S. 229 (2011)	9
<i>Heien v. North Carolina</i> , 135 S. Ct. 530 (2014)	7
<i>Herring v. United States</i> , 555 U.S. 135 (2009)	9, 13, 14
<i>In re Search Warrants Executed on: 309 Primrose Lane</i> , 2007 WL 9775647 (M.D. Pa. Aug. 13, 2007)	20
<i>Lara v. Commissioner Pa. State Police</i> , 91 F.4th 122 (3d Cir. 2024)	12
<i>Massachusetts v. Sheppard</i> , 468 U.S. 981 (1984)	15, 16
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	8
<i>United States v. \$92,422.57</i> , 307 F.3d 137 (3d Cir. 2002)	19, 23, 24
<i>United States v. Blake</i> , 868 F.3d 960 (11th Cir. 2017)	21
<i>United States v. Christine</i> , 687 F.2d 749 (3d Cir. 1982)	23

<i>United States v. Eller</i> , 2023 WL 395938 (9th Cir. 2023)	24
<i>United States v. Getgen</i> , 2011 WL 5826613 (M.D. Pa. Nov. 18, 2011)	17, 20
<i>United States v. Goldstein</i> , 914 F.3d 200 (3d Cir. 2019)	10
<i>United States v. Graves</i> , 751 F. App'x 161 (3d Cir. 2018)	16
<i>United States v. Hodge</i> , 246 F.3d 301 (3d Cir. 2001)	9, 11, 12
<i>United States v. Jarmon</i> , 14 F.4th 268 (3d Cir. 2021)	7
<i>United States v. Katzin</i> , 769 F.3d 163 (3d Cir. 2014)	9
<i>United States v. Leon</i> , 468 U.S. 897 (1984)	9, 12
<i>United States v. McCall</i> , 84 F.4th 1317 (11th Cir. 2023)	10, 19, 21
<i>United States v. Miller</i> , 425 U.S. 435 (1976)	8
<i>United States v. Perez</i> , 280 F.3d 318 (3d Cir. 2002)	25
<i>United States v. Purcell</i> , 967 F.3d 159 (2d Cir. 2020)	21, 22
<i>United States v. Scarfo</i> , 41 F.4th 136 (3d Cir. 2022)	7
<i>United States v. Stabile</i> , 633 F.3d 219 (3d Cir. 2011)	19, 25

United States v. Wright,
777 F.3d 635 (3d Cir. 2015) 16

United States v. Zelaya-Veliz,
___ F.4th ___, 2024 WL 650818 (4th Cir. 2024)..... 10

Walker v. Coffey,
956 F.3d 163 (3d Cir. 2020) 8

Walker v. Coffey,
905 F.3d 138 (3d Cir. 2018) 11

Statutes

18 U.S.C. § 2703..... 7

18 U.S.C. § 2708..... 7

The Court should deny Defendant Donnie Woods' motion to suppress (Doc. 48). The good-faith exception—for multiple independent reasons—precludes the suppression of evidence obtained pursuant to a search warrant for the Apple iCloud account matteww10@icloud.com. Even assuming otherwise, Woods would at most be entitled to severance of the objectional portion of the warrant and the suppression of corresponding evidence. And even if complete suppression were required, Woods' fruit-of-the-poisonous-tree argument is meritless.

PROCEDURAL AND FACTUAL BACKGROUND

In November 2022, a grand jury returned an indictment charging Woods, Danny Fontno, Jr., and Shante Davis with conspiring to distribute fentanyl from July 2020 through April 2021, in violation of 21 U.S.C. § 846.¹ Doc. 1.

The charge was based on a DEA, U.S. Postal Inspection Service (USPIS), and Pennsylvania State Police (PSP) investigation into a drug-trafficking organization that was shipping large quantities of fentanyl

¹ The indictment also charged Fontno and Davis with attempting to possess fentanyl with the intent to distribute. Doc. 1.

into the Middle District of Pennsylvania. Doc. 49-1, at 18-19.² In the early stages of the investigation and in connection with the seizure of about two kilograms of fentanyl that was sent to a residence in Lebanon, Pennsylvania, the DEA obtained a phone number that was connected to the organization, (619) 841-8043. *Id.* at 18-20. That number, in turn, was associated with an Apple subscriber “Matthew [sic] Woods,” who had an iCloud Apple ID of matteww10@icloud.com. *Id.* at 20.

On October 22, 2020, DEA Special Agent Justin Waynick submitted an application for a warrant to search and seize certain items on the matteww10 iCloud account. Doc. 49-1, at 2. The warrant application included an Attachment A, which identified the target iCloud account. *Id.* at 3. The application also included an Attachment B, which identified the things to be seized. *Id.* at 4. Attachment B was divided into two subsections: section I covered “Information to be

² Document 49-1 contains the exhibits Woods filed with his brief in support of his motion to suppress. Page citations are to the pages of the complete PDF.

disclosed by Apple” and section II covered “Information to be seized by the government.” *Id.* at 4-10.

Magistrate Judge Schwab issued the warrant the same day the application was submitted. Doc. 49-1, at at 33. The warrant included the same Attachment A that was submitted with the application. *Id.* at 35. The warrant also included Attachment B, but only section I. *Id.* at 36-40. It did not include section II, which had been the last two pages of Attachment B.

Special Agent Waynick received materials from Apple in response to the matteww10 warrant in December 2020. Doc. 49-1, at 60.

In April 2021, USPIS obtained warrants to search two parcels that were sent from California to 329 East Locust Street in York, Pennsylvania. Doc. 49-1, at 54. One parcel contained about one kilogram of tramadol, and the other parcel contained about three kilograms of fentanyl. *Id.* The DEA, USPIS, and PSP then conducted a controlled delivery to 329 East Locust Street of the parcel that had contained fentanyl. *Id.* After the parcel was taken inside, law enforcement executed a search warrant at the residence. *Id.* at 55. Law enforcement encountered Fontno and Davis and seized \$2,050 and

four phones. *Id.* Through an ion scan, the cash tested positive for a high presence of narcotics, specifically cocaine. *Id.* at 55-56.

In connection with the investigation into the parcels destined for 329 East Locust Street, USPIS obtained records related to inquiries made for parcels that either contained drugs or significant amounts of cash or were otherwise suspicious. Doc. 49-1, at 56-57. Those records revealed, among other things, inquiries associated with the iCloud accounts danfont92@icloud.com and jamesjones317@icloud.com. *Id.* at 57.

On April 28, 2021, Special Agent Waynick submitted applications for and obtained warrants for the four phones seized from 329 East Locust Street. Doc. 49-1, at 76. The next day, he submitted applications for and obtained warrants for the danfont92@icloud.com, jamesjones317@icloud.com, and matteww10@icloud.com accounts. *Id.* at 84, 94, 104. In support of probable cause, Special Agent Waynick provided information about the 329 East Locust Street operation, the USPIS records related to parcel inquiries, the identification of the matteww10 account (which had been included in the original October

2020 warrant), and some communications that were obtained from the original matteww10 warrant. *Id.* at 53-63, 117-26.

Woods filed a motion to suppress the evidence obtained from the original matteww10 warrant based on the omission of section II of Attachment B. Doc. 48. He also seeks to suppress evidence obtained from the warrants issued on April 28 and 29, 2021, on the ground that the evidence is fruit of the original warrant. *Id.*

QUESTIONS PRESENTED

I. Whether the good-faith exception precludes suppression of electronically stored evidence possessed and provided by a third party.

II. Whether the good-faith exception precludes suppression because the omission of section II from Attachment B was due to a clerical error.

III. Whether the good-faith exception precludes suppression because a reasonable officer would have believed that he could seize all of the data provided by Apple.

IV. Whether, at most, severance or redaction is the only appropriate remedy.

V. Whether evidence obtained pursuant to the warrants issued on April 28 and 29, 2021, should not be suppressed.

ARGUMENT

I. The good-faith exception precludes suppression of electronically stored evidence possessed and provided by a third party.

The Fourth Amendment provides, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” As the text

suggests, “the ultimate touchstone of the Fourth Amendment is ‘reasonableness.’” *Heien v. North Carolina*, 135 S. Ct. 530, 536 (2014). Accordingly, the Amendment “protects information in which one has a reasonable expectation of privacy.” *United States v. Jarmon*, 14 F.4th 268, 272 (3d Cir. 2021) (quotation marks omitted). “This requires the defendant to subjectively believe the information is private and for that belief to be objectively reasonable.” *Id.*

It is unclear whether and to what extent an individual has an objectively reasonable expectation of privacy in electronically stored information—like the iCloud data at issue here—that is possessed by a third party.³ “[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the

³ As reflected in Special Agent Waynick’s affidavit, the matteww10 warrant was sought pursuant to provisions of the Stored Communications Act. Doc. 49-1, at 14. That statute requires that the Government secure a warrant to obtain certain types of electronic information stored by certain entities. *See, e.g.*, 18 U.S.C. § 2703(a). The Act does not provide a suppression remedy for violations. *See* 18 U.S.C. § 2708; *United States v. Scarfo*, 41 F.4th 136, 168 n.22 (3d Cir. 2022).

confidence placed in the third party will not be betrayed.” *United States v. Miller*, 425 U.S. 435, 443 (1976); *see also Smith v. Maryland*, 442 U.S. 735, 745-46 (1979) (no legitimate expectation of privacy in phone numbers dialed). Consistent with this third-party doctrine, the Third Circuit has stated that “[p]roviders of electronic communications act as third parties that store and process their users’ private files, meaning the provider-maintained files fall outside Fourth Amendment protection.” *Walker v. Coffey*, 956 F.3d 163, 166 (3d Cir. 2020).

To be sure, in *Carpenter v. United States*, 585 U.S. 296 (2018), the Supreme Court held that the third-party doctrine does not apply to cell-site location information and that “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through” that information. *Id.* at 309-10. But that holding was based on the “unique nature of cell phone location records.” *Id.* at 309. In declining to apply the doctrine, moreover, the Court emphasized the “special solicitude for location information” that it had already recognized in “the third-party context.” *Id.* at 314. And the Court noted that its decision “is a narrow one” that did not disturb the third-party doctrine as set out in *Miller* and *Smith*. *Id.* at 316. The

Court, in short, did not address data beyond cell-site location information.

This Court need not decide whether Woods had a reasonable expectation of privacy in his iCloud data stored by Apple because, at a minimum, the good-faith exception applies. The good-faith rule provides that the exclusion of evidence is appropriate only when given “all of the circumstances,” “a reasonably well trained officer would have known that the [conduct] was illegal.” *United States v. Katzin*, 769 F.3d 163, 182 (3d Cir. 2014) (en banc) (quoting *United States v. Leon*, 468 U.S. 897, 922 n.23 (1984)). The rule reflects the well-established fact that even where a Fourth Amendment violation occurs, exclusion of the obtained evidence is the “last resort,” not the “first impulse.” *Herring v. United States*, 555 U.S. 135, 140 (2009) (internal quotation marks omitted). The “exception requires objectively, not subjectively, reasonable conduct.” *United States v. Hodge*, 246 F.3d 301, 309 (3d Cir. 2001) (Alito, J.). And “searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule.” *Davis v. United States*, 564 U.S. 229, 232 (2011).

Here, a reasonably well-trained officer would not have known whether a warrant satisfying all Fourth Amendment requirements is necessary to obtain electronically stored data possessed by a third party. Although in recent years federal courts have generally concluded that “private electronic communications” are “protected by the Fourth Amendment, even when transmitted over third-party platforms,” neither the Supreme Court nor the Third Circuit has reached that conclusion. *United States v. Zelaya-Veliz*, ___ F.4th ___, 2024 WL 650818, *8 (4th Cir. 2024); *cf. United States v. McCall*, 84 F.4th 1317, 1324 (11th Cir. 2023) (assuming without deciding “that law enforcement must secure a warrant before searching an iCloud account that is held by a third party”). “Only *binding* appellate precedent is relevant to the good faith exception.” *United States v. Goldstein*, 914 F.3d 200, 205 (3d Cir. 2019) (emphasis in original). Because this issue is unsettled in the Third Circuit—and particularly in light of statements in *Walker* that the Fourth Amendment does not protect provider-maintained electronic files—the good-faith exception applies.

The Third Circuit’s decision in an earlier iteration of *Walker* is instructive. The court considered whether qualified immunity shielded

law enforcement from liability for obtaining an employee's work emails without a warrant. *Walker v. Coffey*, 905 F.3d 138, 144 (3d Cir. 2018).

In concluding that the Fourth Amendment right was not clearly established, the court explained that content of communications “is not categorically protected” and that “content that is turned over to a third party is not subject to a reasonable expectation of privacy.” *Id.* at 146.

Because a reasonable officer would not have known whether evidence obtained from a third-party electronic-service provider is covered by the Fourth Amendment, suppression is not proper in these circumstances.

II. The good-faith exception precludes suppression because the omission of section II from Attachment B was due to a clerical error.

The good-faith exception precludes suppression for a second reason. Even assuming the data obtained from the matteww10 account is covered by the Fourth Amendment, any deficiency in the warrant was due to a clerical error.

“The mere existence of a warrant typically suffices to prove that an officer conducted a search in good faith and justifies application of the good faith exception.” *Hodge*, 246 F.3d at 307-08. Suppression of

evidence obtained pursuant to a warrant should be ordered only in “unusual cases.” *Leon*, 468 U.S. at 918. The Third Circuit has identified four “situations in which an officer’s reliance on a warrant would not be reasonable and would not trigger the exception”: (1) the magistrate judge “issued the warrant in reliance on a deliberately or recklessly false affidavit”; (2) the magistrate judge “abandoned his judicial role and failed to perform his neutral and detached function”; (3) “the warrant was based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable”; or (4) “the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized.” *Hodge*, 246 F.3d at 308 (quotation marks omitted).

Woods argues that the fourth situation applies here and prevents application of the good-faith exception.⁴ Doc. 49, at 15. He is incorrect.

⁴ Woods also states in a footnote that the warrant affidavit “provides a very thin reed to support an invasive digital search,” suggesting that the good-faith exception should not apply because the warrant was so lacking in probable cause. Doc. 49, at 15 n.3. “Arguments raised in passing (such as in a footnote), but not squarely argued, are considered forfeited.” *Lara v. Commissioner Pa. State Police*, 91 F.4th 122, 140 n.28 (3d Cir. 2024) (cleaned up). In any event, the affidavit provided

The omission of section II of Attachment B was not the result of any action—deliberate or otherwise—by the affiant, Special Agent Waynick. The exclusionary rule applies “only where it results in appreciable deterrence.” *Herring*, 555 U.S. at 141 (cleaned up). The Supreme Court has accordingly held that a mistake by a court employee does not give rise to exclusion.⁵ *Arizona v. Evans*, 514 U.S. 1, 14 (1995). In justifying this result, the Court explained, “The exclusionary rule was crafted to curb police rather than judicial misconduct; court employees [are] unlikely to try to subvert the Fourth Amendment; and most important, there [is] no basis for believing that application of the

more than sufficient evidence to support probable cause and certainly enough to justify the good-faith exception. The matteww10 iCloud account was associated with the phone number (619) 841-8043. Doc. 49-1, at 20. That number had been identified by an informant as a number associated with someone who delivered drug proceeds to York. *Id.* at 18-19. And this information was corroborated by frequent contacts between that number and a known drug trafficker at around the time the drug trafficker expected to receive two kilograms of fentanyl. *Id.* at 19-20.

⁵ In *Herring*, the Court likewise held that a clerical error by a law enforcement employee should also not result in exclusion. 555 U.S. at 137.

exclusionary rule in those circumstances would have any significant effect in deterring the errors.” *Herring*, 555 U.S. at 142 (cleaned up).

Here, the omission of section II was plainly the result of a clerical oversight at some point during the transmission and finalizing of the warrant by the U.S. Attorney’s Office and the Clerk’s Office, and the omission was most likely due to a simple mistake when the Clerk’s Office scanned the final version of the warrant. Indeed, the docket indicates that Judge Schwab received, reviewed, and approved the entire warrant package, including the complete Attachment B. *See USA/DEA v. Information Associated with Matteww10@ICLOUD.COM*, No. 1:20-mc-570, Doc. 3 (Oct. 22, 2020) (warrant application with the complete Attachment B). That the complete Attachment B did not get filed with the warrant was an inadvertent error and was not the fault of Special Agent Waynick. Exclusion is therefore improper.⁶

⁶ Woods is incorrect that the same error is present for the subsequent matteww10 warrant and the other iCloud warrants issued on April 29, 2021. *See* Doc. 49, at 18, 25; Doc. 49-1, at 147. The dockets for those warrants show that the warrants included the complete Attachment B. *See USA/DEA v. Information Associated with Matteww10@iCloud.com*, No. 1:21-mc-354, Doc. 5 (Apr. 29, 2021); *USA/DEA v. Information Associated with Jamesjones10@iCloud.com*, No. 1:21-mc-353, Doc. 5

This result is confirmed by *Massachusetts v. Sheppard*, 468 U.S. 981, 990-91 (1984), which addressed an analogous mistake. Police sought to obtain a search warrant for a residence to uncover evidence related to a murder. *Id.* at 984-85. Because it was a Sunday, police had trouble finding an appropriate warrant application form and ultimately used a form that had been used previously in a controlled substance investigation. *Id.* at 985. When the detective presented the warrant form to the judge, the two discussed that changes would need to be made to the form, and the judge stated that he would make the necessary changes. *Id.* at 986. The judge made some changes, but he did not change what law enforcement was authorized to search for and seize. *Id.* That portion of the form still covered drug evidence and not the murder evidence. *Id.* at 986 & n.2. In short, as Woods alleges here, the warrant did not particularly describe the items to be seized due to a mistake by someone other than the affiant. A unanimous Supreme

(Apr. 29, 2021); *USA/DEA v. Information Associated with Dafont92@iCloud.com*, No. 1:21-mc-352, Doc. 5 (Apr. 29, 2021). Thus, Woods' standalone claim that evidence obtained pursuant to the April 29 matteww10 warrant should be suppressed is meritless. *See* Doc. 49, at 25.

Court held that the good-faith rule applied. *Id.* at 987-88. The Court explained, “Suppressing evidence because the judge failed to make all the necessary clerical corrections despite his assurances that such changes would be made will not serve the deterrent function that the exclusionary rule was designed to achieve.” *Id.* at 990-91. A similar analysis applies here. Suppressing evidence because a clerical mistake omitted two pages when Attachment B was filed would not serve a deterrent function, and exclusion should not apply.

The impropriety of exclusion is further supported by *United States v. Wright*, 777 F.3d 635 (3d Cir. 2015). A warrant authorizing the search of an apartment identified the items to be seized by referring to an attached affidavit. *Id.* at 637. But before the warrant was transmitted to the affiant, the affidavit was removed and sealed at the request of the U.S. Attorney’s Office, resulting in the affiant receiving a warrant that did not list the items to be seized. *Id.* The Third Circuit applied the good-faith exception, explaining that “detering isolated negligence is not worth the social cost of excluded evidence.” *Id.* at 642; *see also United States v. Graves*, 751 F. App’x 161, 165 (3d Cir. 2018) (no exclusion where warrant mistakenly did not indicate the items to be

seized and did not incorporate an attachment that listed the items); *United States v. Getgen*, 2011 WL 5826613, at *9 (M.D. Pa. Nov. 18, 2011) (Conner, J.) (“The defects in [the warrant] alleged by Getgen involve at most negligent drafting errors, that, if material, relate to hypertechnical constitutional intricacies that would not be fully appreciated by a nonlawyer.”). There is no reason for a different result here.

As compared to cases like *Sheppard* and *Wright*, application of the good-faith exception makes even more sense in the circumstances present here. Apple received all the information it needed—that is, it received Attachment A, which specified the target account; and it received the portion of Attachment B that specified the data it was required to provide. Doc. 49-1, at 35-40. Section II of Attachment B specified what law enforcement should then do with that data and was simply irrelevant for Apple’s purposes. The inadvertent omission of section II simply had no practical consequence and should not result in suppression.

III. The good-faith exception precludes suppression because a reasonable officer would have believed that he could seize all of the data provided by Apple.

The good-faith exception precludes suppression for a third reason. In the circumstances of this case, a reasonably well-trained officer would have believed it was permissible to seize the data covered by section I of Attachment B.

Woods argues that the matteww10 warrant violated the Fourth Amendment's particularity requirement. The Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Woods asserts that the warrant—by inadvertently including only section I of Attachment B—did not describe with sufficient particularity the materials to be seized. Doc. 49, at 9. He specifically notes that section I does not identify the suspected crime or limit the search to any particular time period. *Id.*

This argument fails because the Attachment B as issued by Judge Schwab, although expansive, listed specific items to be provided by

Apple and would not have been viewed as impermissibly overbroad by a reasonably well-trained officer. Multiple cases confirm this fact.

In *United States v. Stabile*, 633 F.3d 219 (3d Cir. 2011), the Third Circuit rejected the argument that the seizure of six entire computer hard drives was unconstitutional. The court explained that “a broad seizure was required because evidence of financial crimes could have been found in any location on any of the six hard drives, and this evidence very likely would have been disguised or concealed somewhere on the hard drive.” *Id.* at 234. The same is true for the drug crimes investigated here, particularly since the sought-after evidence included the identity of the matteww10 accountholder and any other individuals who used or controlled the account. That evidence could exist essentially anywhere in the account data, and section I’s authorization to obtain most of that data would not have rendered the warrant impermissibly overbroad to a reasonable officer. *See United States v. \$92,422.57*, 307 F.3d 137, 149 (3d Cir. 2002) (Alito, J.) (reasonable officer would not have viewed as overbroad warrant allowing seizure of all computers to search for “entire categories of legitimate business records”); *McCall*, 84 F.4th at 1327 (“[C]ommunications between

individuals may be stored in various data formats, including voice memos, shared notes folders, or screenshots of conversations in an images folder. Criminals may even change file extensions or otherwise hide files in a format different from their native format.”); *Getgen*, 2011 WL 5826613, at *7 (“[T]he search could not be limited to certain dates or file extensions because computer files can be easily disguised.”); *In re Search Warrants Executed on: 309 Primrose Lane*, 2007 WL 9775647, at *7-8 (M.D. Pa. Aug. 13, 2007) (Conner, J.), *aff’d* 2009 WL 762417 (3d Cir. 2009) (explaining that “the Third Circuit has not expressly adopted the requirement that a warrant specify the crime alleged to meet constitutional muster” and holding that warrant authorizing seizure of all electronic devices was sufficiently particular because “[i]nclusive warrants actually serve the purpose of the Fourth Amendment’s particularity requirement by hindering the exercise of unbridled discretion by executing officers”).

In *McCall*, the Eleventh Circuit considered whether suppression of evidence from an iCloud account was required where the Government conceded that the warrant “fell short of the particularity requirement because it allowed a search of all the conceivable data on the account

without any meaningful limitation.” 84 F.4th at 1328. Even though the categories of data that investigators were authorized to search pursuant to the warrant “encompassed most of the account’s conceivable data,” the court held that the good-faith exception applied. *Id.*; *see also United States v. Blake*, 868 F.3d 960, 975 (11th Cir. 2017) (not suppressing evidence from Facebook warrants that “required disclosure to the government of virtually every kind of data that could be found in a social media account” because “while the warrants may have violated the particularity requirement, whether they did is not an open and shut matter”).

The Second Circuit reached a similar result in *United States v. Purcell*, 967 F.3d 159 (2d Cir. 2020), in which the court considered a warrant for a Facebook account. In line with Woods’ objections here, the warrant neither identified the offense under investigation nor provided a temporal limitation. *Id.* at 175. Although the warrant essentially required Facebook to provide “virtually all data associated” with the account, the Second Circuit held that the good-faith exception applied because the warrant “identified the target Facebook account to be searched and the specific kinds of data from that account to be

seized.”⁷ *Id.* at 181. The court also explained that law enforcement “obtained the same data from the . . . Facebook account that it would have obtained if the warrant had complied with the Fourth Amendment’s particularity requirement by specifying the relevant offense.” *Id.* at 182. The same analysis applies here.

Because a reasonable officer would not have viewed section I of Attachment B as impermissibly overbroad, the good-faith exception precludes suppression.

IV. Severance or redaction is the only appropriate remedy.

Even assuming that the matteww10 warrant is overbroad and that the good-faith rule does not apply, suppression of all evidence obtained pursuant to the warrant is not proper. Rather, an overly broad warrant should be cured by “striking from [the] warrant those

⁷ As examples of the broad categories of data requested, the court noted that the warrant affidavit listed “subscriber information and contact information; a user neo-print including historical log-in data and postings made to the target account[]; a photo-print including both saved and deleted photographs posted by the target account[’s] users, photographs in which the target account[] w[as] tagged, and all associated metadata; any public or private messages; IP logs; all chat history, including content of all chats and date and time information; and all searches data.” 967 F.3d at 173-74 (cleaned up).

severable phrases and clauses that are invalid for lack of probable cause or generality and preserving those severable phrases and clauses that satisfy the Fourth Amendment.” *United States v. Christine*, 687 F.2d 749, 754 (3d Cir. 1982). “Each part of the search authorized by the warrant is examined separately to determine whether it is impermissibly general or unsupported by probable cause. Materials seized under the authority of those parts of the warrant struck for invalidity must be suppressed, but the court need not suppress materials seized pursuant to the valid portions of the warrant.” *Id.* This remedy appropriately recognizes that the “cost of suppressing all the evidence seized, including that seized pursuant to the valid portions of the warrant, is so great that the lesser benefits accruing to the interests served by the Fourth Amendment cannot justify complete suppression.” *Id.* at 758.

The Third Circuit’s decision in *United States v. \$92,422.57* is instructive. The court considered a warrant that authorized the seizure of a broad set of records from a business, including all computers. 307 F.3d at 144. In rejecting the argument that the warrant should have narrowly limited the relevant time period, the Third Circuit explained

that the inclusion of additional years “simply authorized a search for documents as to which there may not have been probable cause.” *Id.* at 151. “The proper remedy . . . was simply to excise the years for which there was no probable cause.” *Id.* Thus, even if the Court concludes that the warrant as issued by Judge Schwab was overbroad, the remedy is to limit the Government’s evidence to the evidence for which there was clearly probable cause—at a minimum, evidence related to drug trafficking in 2020. *See United States v. Eller*, 2023 WL 395938, at *1 (9th Cir. 2023) (no suppression because the evidence at issue was from a period “for which the warrant affidavit gave probable cause and is therefore sufficiently specific and particular to support severance”) (quotation marks omitted).

V. Evidence obtained pursuant to subsequent warrants should not be suppressed.

Even assuming that all of the evidence from the initial matteww10 warrant must be suppressed, the fruit-of-the-poisonous-tree doctrine does not require suppression of evidence seized pursuant to warrants issued on April 28 and 29, 2021.

The April 28 warrants sought to search four phones that were seized from 329 East Locust Street in York on April 16, 2021. Doc. 49-1, at 42. The April 29 warrants sought to search three iCloud accounts: danfont92@icloud.com, jamesjones10@icloud.com, and matteww10@icloud.com. *Id.* at 84, 94, 103.

The fruit-of-the-poisonous-tree doctrine typically requires the suppression of evidence obtained as a result of an illegal search. *Stabile*, 633 F.3d at 243. But the independent-source doctrine serves as an exception to the exclusionary rule and allows the introduction of evidence obtained pursuant to a subsequent warrant if (1) “a neutral justice would have issued the search warrant even if not presented with information that had been obtained during an unlawful search” and (2) “the first search [did not] prompt[] the officers to obtain the subsequent search warrant.” *Id.* (cleaned up). “The basis for [this] rule is the well-established principle that evidence is not to be excluded if the connection between the illegal police conduct and the discovery of the evidence is so attenuated as to dissipate the taint.” *United States v. Perez*, 280 F.3d 318, 338 (3d Cir. 2002) (quotation marks omitted).

Woods is incorrect that the material from the initial matteww10 warrant was essential to probable cause for the April 28 and 29, 2021, warrants. Those warrants were based on the following evidence, which was independent from the matteww10 material.⁸

- On August 28, 2020, USPIS executed a warrant on a parcel sent from California to 133 Lehman Street in Lebanon, Pennsylvania. Doc. 49-1, at 58. Law enforcement recovered approximately two kilograms of fentanyl. *Id.* They then conducted a controlled delivery of the parcel to 133 Lehman Street and executed a search warrant at the residence. *Id.* They recovered nearly \$150,000 in drug proceeds, drug ledgers, receipts for numerous wire transfers to the Dominican Republic, and a firearm. *Id.* They also recovered the resident's phone, which had the number (646) 427-1952. *Id.*

⁸ The citations in the below summary are to the affidavit supporting the April 28 warrants for the four phones. The affidavit supporting the April 29 warrants for the three iCloud accounts contained the same information. Doc. 49-1, at 117-23.

- Toll records for the 1952 phone showed eight contacts from that phone to (619) 841-8043 from August 26 through 29, 2020. *Id.* at 59.
- A confidential source identified a subject residing in Mexico who coordinated the shipping of fentanyl and the remittance of drug proceeds to and from central Pennsylvania, as well as other areas of the country. *Id.* at 53. The source identified the 8043 phone as a phone associated with a male who coordinated the delivery of drug proceeds to York on or about August 29, 2020. *Id.* at 53-54, 59.
- An Apple subpoena response indicated that the 8043 number was associated with the Apple subscriber “Matthew [sic] Woods” with an iCloud Apple ID of matteww10@icloud.com. *Id.* at 59.
- In April 2021, USPIS obtained search warrants for two parcels sent from California to 329 East Locust Street in York. *Id.* at 54. USPIS recovered over one kilogram of tramadol from one parcel and over three kilograms of fentanyl from the other parcel. *Id.*

- Law enforcement then conducted a controlled delivery of the parcel that had contained fentanyl to 329 East Locust Street. *Id.* After the parcel was delivered, Shante Davis brought it inside the house. *Id.* at 55. Danny Fontno, Jr., was also in the house that day. *Id.* Later in the day, law enforcement executed a search warrant at the residence. *Id.* They found the parcel in the second-floor master bedroom. *Id.* They also found \$2,050 and the four phones that would later be the targets of the April 28 warrants. *Id.* Through an ion scan, the money tested positive for a high presence of narcotics, specifically cocaine. *Id.* at 56. Davis said that she owned the residence and that only she and a small child lived there. *Id.* Fontno denied owning any of the phones and identified one as belonging to Davis. *Id.* Davis was arrested and charged with state drug crimes, and Fontno was released. *Id.*
- Postal records indicated that inquiries regarding the parcels destined for 329 East Locust Street were made by the phone number (717) 882-7097 and the email address danfont31@gmail.com. *Id.* The phone number and email

address had contacted the Postal Service on April 12, 2021, about the status of the package containing fentanyl. *Id.*

- The 7097 number had also inquired about other parcels. *Id.* One parcel had been seized by USPIIS in March 2021, and law enforcement recovered nearly \$40,000, which was being sent from York to Los Angeles. *Id.* at 56-57. The email address associated with that inquiry was danfont92@icloud.com. *Id.* at 57.
- The 7097 number was also connected with an inquiry regarding a parcel sent from California to Ephrata, Pennsylvania, in December 2020. *Id.* The email address associated with the inquiry was jamesjones317@icloud.com. *Id.*
- The jamesjones317@icloud.com address was connected to an inquiry regarding a parcel that was delivered in August 2020 to 224 West College Avenue in York, with a sender address in California. *Id.* The phone number (404) 988-7735 was also associated with this inquiry. *Id.* The sender address for this parcel was almost identical to the sender address of the

two parcels that were destined for 329 East Locust Street in April 2021. *Id.* at 54, 57.

This evidence provided a more than sufficient basis to believe that evidence of drug trafficking would be found on the four phones and the iCloud accounts of jamesjones317@icloud.com, danfont92@icloud.com, and matteww10@icloud.com. The information obtained from the initial matteww10 warrant that was included in the supporting affidavits was limited. It merely established a connection between Fontno and the matteww10 account, indicating that the two had communicated regarding two parcels using vague or coded language.⁹ Doc. 49-1, at 60-61.

Woods is correct that the matteww10 materials recounted in the affidavits provided relevant evidence. Doc. 49, at 29. But that evidence was not necessary to provide probable cause to search the four phones and three iCloud accounts. Rather, the evidence summarized at length

⁹ Woods is simply wrong when he says that the affidavits included “a lengthy and detailed account” of the contents of the matteww10@icloud.com account. Do. 49, at 23. The affidavits included a handful of messages between Matthew Woods and the 7735 number. Doc. 49-1, at 60-62.

above established probable cause and was crucial since it involved actual seizures of drugs and cash. The purpose of the mattheww10 materials was to merely establish a connection between what could have been seen as two separate operations and to provide additional (but unnecessary) evidence related to Fontno. That the evidence summarized above independently established probable cause is supported by multiple facts.

First, probable cause that Fontno was engaged in a drug-trafficking conspiracy was established by Fontno's presence with only one other adult in a house that was supposed to receive three kilograms of fentanyl and one kilogram of tramadol; his denial that any of the phones in the residence belonged to him; the inquiry by danfont31@gmail.com about the parcels; the inquiry by danfont92@icloud.com related to a parcel that contained almost \$40,000; and Fontno's connection to the 7097 phone, which made inquiries into packages that contained drugs or large amounts of money. Doc. 49-1, at 54-57.

Second, the affidavits established that Davis was involved in a drug-trafficking conspiracy, but she was not mentioned in the summary of the matteww10 materials.

Third, the affidavits did not provide numbers for the four target phones or purport to establish that any of the phones were involved in the communications retrieved from the matteww10 account. In other words, probable cause to search the phones was based primarily on their presence at a house that was meant to receive three kilograms of fentanyl and one kilogram of tramadol as well as Special Agent Waynick's general training and experience that cell phones possessed by drug traffickers often contain historical records of drug-trafficking activities.

Fourth, both the danfont92@icloud.com account and the jamesjones317@icloud.com account made inquiries into suspicious packages and were connected to the 7097 phone. Doc. 49-1, at 56-57. That phone was associated with the inquiries of the parcels sent to 329 East Locust Street as well as the parcel that contained nearly \$40,000. *Id.* Thus, probable cause to search those iCloud accounts existed

without the matteww10 materials, and indeed, the jamesjones317 account was not mentioned in the summary of those materials.

Fifth, the April 29 affidavit reprised the same evidence as the original October 2020 matteww10 affidavit, and that first affidavit established probable cause to search the account. *Compare* Doc. 49-1, at 18-20, *with id.* at 53-54, 58-59.

Thus, probable cause would have supported the April 28 and 29 warrants even without the original matteww10 materials. Law enforcement, moreover, would have obtained those warrants even had they not obtained the original matteww10 materials. The warrants followed the USPIS seizure of significant quantities of drugs that were destined for 329 East Locust Street in York. That event—rather than the DEA’s receipt of the matteww10 materials months earlier—prompted law enforcement to obtain the additional warrants.

Because the April 28 and 29 warrants were sufficiently attenuated from any potential illegality in obtaining the original matteww10 warrant, there is no basis to suppress evidence obtained pursuant to the April 28 and 29 warrants.

CONCLUSION

The Court should deny Woods’ motion to suppress. No hearing is necessary if the Court holds that the good-faith exception precludes suppression because the evidence was provided by a third party or because an officer could have reasonably believed that section I of Attachment B was not impermissibly overbroad. Those applications of the good-faith exception—as set forth in sections I and III above—are based on facts that Woods does not appear to dispute.

Dated: March 12, 2024

Respectfully submitted,

GERARD M. KARAM
United States Attorney

/s/ Carlo D. Marchioli
Carlo D. Marchioli
Assistant U.S. Attorney
PA 309217
United States Attorney’s Office
Middle District of Pennsylvania
Sylvia H. Rambo U.S. Courthouse
1501 North 6th Street, Box 202
Harrisburg, PA 17102
Tel: (717) 221-4482
carlo.d.marchioli@usdoj.gov

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the Court's order of January 31, 2024 (Doc. 47) because it contains 6,180 words. That order granted Woods' motion to file a supporting brief not to exceed 25 pages and provided that "[t]he government in its response may likewise file a brief of this length." This brief and Woods' brief are formatted differently, making it infeasible to compare pagination. Woods' brief, however, contained 7,982 words.

/s/ Carlo D. Marchioli
Carlo D. Marchioli
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I certify that on March 12, 2024, I served the foregoing document
by electronic service on the following individual:

James Maguire, Esq.
maguire@wisemanschwartz.com

/s/ Carlo D. Marchioli
Carlo D. Marchioli
Assistant U.S. Attorney